THE CENTER FOR
INTERNET SECURITY SM

The Business Case
for
Secure Products

Clint Kreitner
www.cisecurity.org
ckreitner@cisecurity.org

I hear managers everywhere asking :

- What do I need to do?
- How much is enough?
- Who can I trust?
- How can I resolve the conflicting advice I'm receiving from "the experts"?

“How can I get beyond this cycle of failure?”

- A break in occurs
- A well-known vulnerability was exploited
- Security staff and system administrators argue about who was to blame
- Senior management sees the process as broken
- Staffs are reorganized; managers are reassigned
- The new managers hire a consultant to do a vulnerability analysis and penetration test

So...

- The consultant’s analysis shows an average of up to 30 vulnerabilities per system
- Management writes a memo telling system administrators and department heads to fix these vulnerabilities within xx weeks
- The work would take months; system administrators don’t make all the fixes – not even a small fraction. At the same time new software is installed; new vulnerabilities are created

And then again…

- Anther break in occurs
- A well-known vulnerability was exploited
- Security staff and system administrators argue again…
- Senior management sees the process as broken

Why are vendors shipping unsecured systems?

- "Our customers don't want security; they want features and performance. When they do want security, we'll deliver it."
- "Every customer wants something different. We can't be expected to deliver and maintain thousands of different configurations."

Three years ago a large cohort of users said, “We want to:

- Speak to vendors/OEM’s with a single voice to make it clear that we:
  - Value security
  - Can agree on what defines a safer baseline configuration.
  - Want to buy safer systems
  - Need a way to measure and monitor our security status on an ongoing basis
  - Plan to begin demanding safer systems”

Users are demanding:

- Fewer defects and better default configurations to:
  - Defend against intrusion
  - Demonstrate due care against potential liability
  - Qualify for insurance premium discounts
  - Reduce the cost of operating IT systems

Challenge to vendors

- You have been way too agnostic about providing products with adequate security baked-in
  - Remember Volvo?
- It's time to listen closely to your customers about their security requirements, especially when they speak with a united voice

Software quality – an oxymoron

- What other manufactured product is shipped with so many defects?
  - In the meantime, make patching easier and safer, and improve your default security configurations

Provide users with a choice of default configuration options for:

- Different security levels
- Different system roles

OS, application, and appliance vendors need to work more closely together

- To test common OS/application combinations for breakage
  - Users don't buy computers to run operating systems
- Appliances
  - Copiers, scanners, printers, etc.

Encouraging progress

- Dell's decision to offer pre-configured W2K systems and plans to offer others
- Top security experts from Microsoft, Sun, HP, Cisco, and Oracle are active on the benchmark teams
- 2003 Server with better defaults
- AOL's decision to work with CIS on an AOL User's benchmark

Vendors have the opportunity to:

- Drag their feet with the tired arguments about adding cost, or
- Become a leader and get out in front of the pack by producing more secure products for their customers
- Work closely with their customers to this end

The business case for security

Vendors who provide secure products to their customers will prosper; those who do not, will not.

Thank you!

dl.ethan@disecurity.org
http://www.disecurity.org